Review of the State of Tennessee's Remediation Efforts for the Year 2000: State Agencies and Institutions of Higher Education

May 1999

Arthur A. Hayes, Jr., CPA
Director

Glen W. McKay, CIA
Assistant Director

Chuck Richardson, CPA, CISA
Audit Manager

Beth Pendergrass, CISA
Audit Manager

Jane Russ
Editor

Will Hancock, CPA
Teresa A. Lawson
Karen R. Masters
Bonnie A. Pauly, CISA
Staff Auditors

Robert L. Rice, CISA
Clementine Williams
Caryn D. Woolley
Staff Auditors

May 31, 1999

The Honorable Don Sundquist, Governor
and
The Honorable John S. Wilder
Speaker of the Senate
The Honorable Jimmy Naifeh
Speaker of the House of Representatives
and
Members of the General Assembly
State Capitol
Nashville, Tennessee 37243

Ladies and Gentlemen:

Transmitted herewith is the review of the State of Tennessee's remediation efforts for the Year 2000. Officials from the State of Tennessee's agencies and institutions of higher education are engaged in remediation efforts designed to address the Year 2000 problem. Remediation efforts include all phases of preparing computer systems and other equipment for Year 2000 operational effectiveness. Significant progress has been made and remediation efforts are continuing. However, certain matters came to our attention that if left uncorrected could diminish the effectiveness of the state's overall remediation efforts:

- Mission-critical application systems reported as remediated by programming staff were not always certified as remediated by owners.
- Few entities reported that they had documented communications regarding interfaces between systems.
- Although inventories of mission-critical application systems had been developed, few entities reported conducting an inventory of embedded systems and performing risk assessments of these systems.
- Most entities reported that they had not established business continuity plans.
- OIR reported the potential for major problems in the remediation efforts for the Administrative Office of the Court's Tennessee Court Information System (TnCIS), the Department of Children's Services Tennessee Kids Information Delivery System (TNKIDS), and the Bureau of TennCare's TennCare Management Information System (TCMIS).

Despite reasonable and diligent efforts by state officials, the ultimate effectiveness of Year 2000 remediation efforts cannot be determined with complete assurance until January 1, 2000. Because of the prevailing uncertainty surrounding the effectiveness of remediation efforts, state officials must continue their diligence in remediating computer systems and other equipment and make appropriate preparations in the event of unanticipated technology failures. Management should review the above observations and take corrective action where indicated.

This review was prepared pursuant to the provisions of Section 4-3-304(6), *Tennessee Code Annotated*, which authorizes the Department of Audit to perform economy and efficiency audits, program results audits, and program evaluations.

Sincerely,

John G. Morgan
Comptroller of the Treasury

JGM/bp
99-705

State of Tennessee

Review Highlights

Comptroller of the Treasury — Division of State Audit

Review Report

Review of the State of Tennessee's Remediation Efforts for the Year 2000: State Agencies and Institutions of Higher Education

May 1999

BACKGROUND

The Year 2000 problem is based on the inability of computer systems to determine whether the two-digit representation for 2000 (00) means 2000 or 1900. Thus, computer systems that use dates for calculations, comparisons, or sorting may fail or may provide inaccurate data when presented with this condition.

The State of Tennessee is engaged in Year 2000 remediation efforts. Remediation efforts include all phases of preparing computer systems and other equipment for Year 2000 operational effectiveness. These phases typically include (1) inventorying systems to determine those that support core business processes affected by the Year 2000, and prioritizing their conversion or replacement; (2) converting, replacing, or eliminating these systems; and (3) testing and verifying converted or replaced systems in an operational environment.

OBJECTIVES

The objectives of the review were to examine the extent to which the State's Year 2000 Project Manager and the Year 2000 Coordinators from the University of Tennessee's University-Wide Administration and the Tennessee Board of Regents have developed an inventory of mission-critical application systems (computer programs that provide fiscal and administrative services) and the status of remediation efforts for those systems. The auditors also sought to develop a comprehensive inventory and the status of remediation efforts for infrastructure components of computer systems, i.e., supporting software systems, hardware, and communications equipment, from state agencies and institutions of higher education. In addition, from state agencies only, the review sought to obtain assessments of the performance of the Office for Information Resources (OIR), Department of Finance and Administration, in providing Year 2000 remediation support services.

METHODOLOGY

The review was performed using surveys, questionnaires, interviews, and reviews of information provided by the Year 2000 Project Manager, Year 2000 Coordinators, and other appropriate staff in state agencies and institutions of higher education. Review efforts focused on the remediation status of mission-critical application systems because of their pervasive effect on government operations. Auditors initially

administered surveys to, and completed standardized questionnaires with, Year 2000 Coordinators and other appropriate staff in 53 state agencies, 20 Tennessee Board of Regents institutions, and seven University of Tennessee institutions between August and October 1998. This effort provided an inventory and the status of remediation for mission-critical application systems and infrastructure components of computer systems as reported by individual Year 2000 Coordinators. Once compiled, this information was provided to the state's Year 2000 Project Manager and Year 2000 Coordinators of the University of Tennessee and the Tennessee Board of Regents in order to corroborate or to supplement their information. Recognizing testing of converted or replaced systems as an essential element of remediation efforts, auditors again questioned Year 2000 Coordinators and other appropriate staff in April 1999 regarding the status of testing for mission-critical applications. The review focused on state agencies and institutions of higher education. No procedures were performed pertaining to the Year 2000 efforts and activities of the federal or local governments or of private-sector third parties.

ANALYSIS AND EVALUATION

Inventories of Mission-Critical Application Systems and Infrastructure Components of Computer Systems Have Been Developed

The state's Year 2000 Project Manager has developed an inventory of mission-critical application systems. Also, the Year 2000 Coordinators of the University of Tennessee and the Tennessee Board of Regents have identified mission-critical application systems (also identified as "essential administrative systems") utilized by all campuses. In addition, the Year 2000 Project Manager and the Year 2000 Coordinators of the University of Tennessee and the Tennessee Board of Regents have compiled inventories of infrastructure components of computer systems. (See pages 10-11.)

Remediation Efforts for Mission-Critical Application Systems and Infrastructure Components of Computer Systems Are in Progress

Mission-Critical Application Systems

Auditors have observed evidence of remediation efforts throughout the review period. Remediation efforts are in progress for state agencies and institutions of higher education and are expected to continue through the end of the current calendar year. Overall, as of January 19, 1999, the Year 2000 Project Manager reported 90% remediation for state agency mission-critical application systems. The Year 2000 Coordinator for the University of Tennessee reported 87% remediation for mission-critical application systems, and the Year 2000 Coordinator for the Tennessee Board of Regents reported 90% remediation for mission-critical application systems. Although the reported percentages indicate that the total work effort for remediation of mission-critical systems is near completion, these percentages are subject to several qualifications which are discussed in detail in the report. The extent of completion of total remediation efforts noted above is based on percentage of total work effort planned, including testing.

Testing is the final phase in the remediation process. The Office for Information Resources (OIR) and the statewide Year 2000 Project Manager had established December 31, 1998, as the target date for renovating mission-critical application systems, so that calendar year 1999 could be used for testing. In April 1999, division staff contacted each Year 2000 Coordinator reporting mission-critical application systems to determine the current status of testing for those systems.

Of the combined 334 mission-critical application systems reported by state agencies and institutions of higher education, testing was either complete or in progress for 90 percent of state agency systems, 100 percent of University of Tennessee systems, and 100 percent of Tennessee Board of Regents systems. The expected completion dates for systems currently undergoing testing ranged from April to October 1999.

These percentages vary from those noted for total remediation since (1) these figures are on a per-system basis, (2) reflect conditions after the above total remediation percentages were obtained, and (3) are limited to the testing phase of remediation. For the 30 remaining state agency systems, testing was planned for 18, and expected completion dates ranged from May to September 1999. Coordinators also reported 12 systems (4 percent of the total 334 mission-critical systems) for which no testing was planned. Coordinators cited the following reasons for not testing these systems: the systems are no longer used or will not be used as of January 1, 2000, or the systems do not process date fields.

Infrastructure Components of Computer Systems

In addition to obtaining an inventory of infrastructure components of computer systems, the auditors' survey was designed to obtain reported remediation status for these components. The results of the survey indicated that overall for mission-critical hardware items, 60% were 100% remediated, for 9% there was some progress, while for 31% there was no measurable progress. For mission-critical other software items, 52% were 100% remediated, for 19% there was some progress, while for 29% there was no measurable progress. For mission-critical communications items, 38% were 100% remediated, for 18% there was some progress, while for 43% there was no measurable progress. Information obtained through the auditors' surveys and questionnaires relating to infrastructure components of computer systems was provided to the state's Year 2000 Project Manager and Year 2000 Coordinators of the University of Tennessee and the Tennessee Board of Regents in order to corroborate or to supplement their information. Remediation efforts are continuing for these components. (See pages 11-16.)

State Agencies Rated the State of Tennessee's Office for Information Resources (OIR's) Year 2000 Support Activities as Excellent or Good

Most state agencies have rated OIR's Year 2000 support activities as excellent or good. The Office for Information Resources (OIR) of the Department of Finance and Administration made information and resources available for agencies to use in making their determinations for the Year 2000 Project Manager about what was needed to make their internal systems Year 2000 ready. Auditors surveyed state agencies to determine their opinions of the Year 2000 support that OIR provided. A majority of agencies rated OIR either excellent or good in each of the areas addressed in the survey. Those areas are as follows: problem awareness, problem assessment, technical assistance, program modifications, program testing, revision implementation, and funding assistance. (See pages 16-17.)

OTHER OBSERVATIONS

The 1998 State of Tennessee Comprehensive Annual Financial Report's Independent Auditor's Report, dated January 25, 1999, included the following statement:

> Because of the unprecedented nature of the year 2000 issue, its effects and the successes of related remediation efforts will not be fully determinable until the year 2000 and thereafter. Accordingly, insufficient audit evidence exists to support the State of Tennessee's disclosures with respect to the year 2000. . . . Further, we do not provide assurance that the State of Tennessee is or will be year 2000 ready, that the State of Tennessee's year 2000 remediation efforts will be successful in whole or in part, or that the parties with which the State of Tennessee does business will be year 2000 ready.

Despite reasonable and diligent efforts by state officials, the ultimate effectiveness of Year 2000 remediation efforts cannot be determined with complete assurance until January 1, 2000. In light of the

possible serious consequences associated with Year 2000 failures, we believe that the following observations relating to Year 2000 remediation efforts should be carefully considered by officials of state agencies and higher education and action taken where indicated.

Mission-Critical Application Systems Reported as Remediated by Programming Staff Were Not Always Certified as Remediated by Owners

Owner agencies are responsible for accepting a system's remediation and certifying the system to OIR as Year 2000 compliant. A review of 327 mission-critical application systems identified 160 remediated systems, of which only 54 had been certified by the owner agencies as Year 2000 compliant. Auditors found 9 additional certification forms that had been altered by the owner agencies such that the certification was inappropriate. OIR should emphasize the importance of submitting certifications of compliance when systems meet the standards and should promptly reject certifications altered by the owner agencies. (See pages 17-18.)

Few Entities Reported That They Had Documented Communications Regarding Interfaces Between Systems

Of the 80 entities responding to the Division of State Audit standardized interview questions, 64 reported that they had interfaces. Of those, 53 (83%) reported that they did not have written agreements with their business partners to ensure Year 2000 data compatibility. "Agreements" in this context means documentation of the agreed-upon format for how shared data was to be transmitted and received. Interfaces transfer data between two or more business partners using electronic media (e.g., transfers from one computer to another using a dedicated network, exchanges over commercially available networks or the Internet, or exchanges of magnetic media such as tapes or disks). Since not all organizations are changing their date fields to address Year 2000 issues in the same way, it is important that formal communications exist between interface partners so that data is compatible and can be transferred accurately and effectively. OIR's standard for interfaces is for all agencies to use a four-digit year field (2000, rather than the two-digit 00).

OIR guidance states that if an existing system cannot comply with the standard yet must exchange data with another system, both entities must agree, in writing, to the date format represented in the application and that both parties keep a copy of this agreement.

According to University of Tennessee officials, the University-Wide Administration (UWA) promulgates data exchange standards for all intercampus interfaces; thus, according to UT officials, interfaces are well documented. UWA generally uses a two-digit year format in conjunction with "windowing" programming techniques to achieve data exchanges. UWA has reportedly documented these requirements along with data exchange requirements with external financial institutions and the state and federal governments.

The Tennessee Board of Regents does not utilize a standard format for date fields.

Although the absence of written agreements does not mean that agency staff have not determined the appropriate date formats to enable interfacing, formal documentation of such determinations would appear appropriate. Such documentation would ensure that appropriate staff have in fact communicated with their data exchange partners and that relevant information has been shared. Management should ensure that communications regarding date formats for transmitting and receiving data are documented. (See pages 18-20.)

Although Inventories of Mission-Critical Application Systems Had Been Developed, Few Entities Reported Conducting an Inventory of Embedded Systems and Performing Risk Assessments of These Systems

Embedded systems are microprocessors (computer chips) found in a vast array of devices such as biomedical equipment, electrical monitoring and distribution devices, communication systems, building security and fire systems, elevators, traffic control and street light systems, automated heating and cooling systems, and office equipment. Of the 80 entities responding to Division of State Audit standardized interview questions, twenty-nine responded Not Applicable to the question, "Do you have an inventory of systems with embedded chips?" Seven responded that they had conducted an inventory of their embedded systems, and 44 answered that they had not conducted an inventory of their embedded systems. On November 13, 1997, OIR instructed agencies to provide to the Year 2000 Project Manager a listing of all of their projects, including embedded systems. OIR requested that agencies provide this information by December 15, 1997, and update it each month. Agencies have provided and are updating listings of their projects as requested.

The Division of State Audit analyzed the current inventory listing submitted to the project manager as of January 19, 1999. Individual agencies are responsible for reporting on embedded systems applicable to their specific needs. Included in the inventory are responses from OIR's telecommunications section and the Department of General Services identifying embedded systems for which they are responsible. Forty-four of 80 entities questioned reported that they had not inventoried their embedded systems. An additional 29 entities responded that an inventory of embedded systems did not apply to them. These 29 entities were state agencies and included the Departments of Agriculture, Correction, Environment and Conservation, Health, and Mental Health and Mental Retardation. Because of the size and multifunctional nature of these departments, it is likely that they do utilize embedded systems.

Just as with application systems and infrastructure components of computer systems, each agency or institution of higher education needs a comprehensive inventory of embedded systems. These inventories would identify embedded systems falling under the authority of OIR, the Department of General Services, or the entity itself. To ensure continuation of services, entities must identify their embedded systems, determine which systems are essential through a risk assessment process, and prepare contingency plans for continuing operations in case essential embedded systems fail. Management should ensure it has prepared comprehensive inventories and performed risk assessments of embedded systems to develop effective contingency plans in case the essential embedded systems fail. (See pages 20-22.)

Most Entities Reported That They Had Not Established Business Continuity Plans

Of the 80 agencies, colleges, and universities responding to Division of State Audit standardized interview questions, 91% did not have business continuity plans. Business continuity planning helps to ensure an entity maintains its critical functions in case of Year 2000-related failures of computer systems and other equipment. Business continuity planning is not an information technology issue. Continuity planning does not involve matters such as developing software "patches" for flawed systems or otherwise rewriting programs or changing system configurations. Instead, planning involves the development of operating procedures to provide continued service delivery in the event of computer systems and other equipment failures. Hence, it should not be necessary to engage those technical staff addressing the Year 2000 remediation efforts in developing these plans to the extent of diverting their primary focus from the technical aspects of the Year 2000 problem. Management should establish a business continuity plan by evaluating the costs and benefits of alternative operating procedures for each critical business process. (See pages 22-24.)

OIR Reported Three Systems Have Potential for Major Problems in Their Remediation Efforts

As of April 1, 1999, OIR's Year 2000 Status Report stated that potential problems were being monitored as needed to ensure all mission-critical applications were successfully remediated. OIR is not directly responsible for the development or conversion of the following systems that were reported as having the potential for major problems:

- Tennessee Court Information System (TnCIS)—The State of Tennessee's Administrative Office of the Courts is developing this new system to replace several different application systems currently in use in the county courts. According to OIR staff, the new system is designed to provide uniformity in reporting and more effective statewide statistical compilation. However, TnCIS will not be implemented by December 31, 1999. Therefore, each of the systems currently in use must be made Year 2000 compliant by their respective vendors. These systems are reportedly in various stages of the remediation process, and the vendors have stated that each existing system will be ready by December 31, 1999. However, the existing systems must be remediated to ensure efficient operation of the courts.
- Tennessee Kids Information Delivery System (TNKIDS)—The Department of Children's Services is developing a new system to provide coordinated services for Tennessee's children and their families, allowing the department to track the children, their needs, and the services they receive. According to OIR, "The Department relies on several very old systems, which are not being remediated. These systems are to be replaced by the new TNKIDS system. This system must be implemented in a timely manner to provide basic business functionality." According to Department of Children's Services staff, a temporary workaround will be in place by May 3, 1999.
- TennCare Management Information System (TCMIS)—The Bureau of TennCare is remediating this system to be Year 2000 compliant with the help of Electronic Data Systems (EDS), the vendor. TCMIS tracks data relating to TennCare clients and the services they receive, as well as payments to providers. According to OIR, "The contractor responsible for this system started remediation efforts very late and has already missed the first critical time frame. A temporary workaround is in place. Failure to complete changes to this system will result in very serious service disruptions."

OIR should continue to monitor progress and provide appropriate guidance relating to these systems. (See pages 24-25.)

"Review Highlights" is a summary of the review report. To obtain the complete review report which contains all analysis and evaluation, recommendations, and management comments, please contact

Comptroller of the Treasury, Division of State Audit
1500 James K. Polk Building, Nashville, TN 37243-0264
(615) 741-3697

REVIEW OF THE STATE OF TENNESSEE'S REMEDIATION EFFORTS FOR THE YEAR 2000: STATE AGENCIES AND INSTITUTIONS OF HIGHER EDUCATION

TABLE OF CONTENTS

	Page
INTRODUCTION	1
Purpose and Authority	1
Objectives	1
Scope and Methodology	1
BACKGROUND INFORMATION	4
The Year 2000 Problem	4
State of Tennessee's Year 2000 Efforts	4
Review Methodology	8
ANALYSIS AND EVALUATION	10
Inventories of mission-critical application systems and infrastructure components of computer systems have been developed	10
Remediation efforts for mission-critical application systems and infrastructure components of computer systems are in progress	11
State agencies rated the State of Tennessee's Office for Information Resources (OIR's) Year 2000 support activities as excellent or good	16
Mission-critical application systems reported as remediated by programming staff were not always certified as remediated by owners	17
Few entities reported that they had documented communications regarding interfaces between systems	18

TABLE OF CONTENTS (CONT.)

Page

ANALYSIS AND EVALUATION (Cont.)

Although inventories of mission-critical application systems had been developed, few entities reported conducting an inventory of embedded systems and performing risk assessments of these systems 20

Most entities reported that they had not established business continuity plans 22

OIR reported three systems have potential for major problems in their remediation efforts 24

APPENDIX 26

U.S. General Accounting Office Guides 26

Review of the State of Tennessee's Remediation Efforts for the Year 2000: State Agencies and Institutions of Higher Education

INTRODUCTION

PURPOSE AND AUTHORITY

This review of the State of Tennessee's remediation efforts for the Year 2000 was prepared pursuant to Section 43-3-304(6), *Tennessee Code Annotated*, which authorizes the Department of Audit to perform economy and efficiency audits, program results audits, and program evaluations. The purpose of the review was to examine the state's Year 2000 remediation efforts based on representations by appropriate staff in state agencies and institutions of higher education.

OBJECTIVES

The following were the objectives of the review:

1. To examine the extent to which the state's Year 2000 Project Manager and the Year 2000 Coordinators from the University of Tennessee's University-Wide Administration and the Tennessee Board of Regents have developed an inventory of mission-critical systems and the status of remediation efforts for those systems.

2. To develop a comprehensive inventory and the status of remediation efforts for infrastructure components of computer systems, i.e., supporting software systems, hardware, and communications equipment, from state agencies and institutions of higher education.

3. To obtain, from state agencies only, assessments of the performance of the Department of Finance and Administration's Office for Information Resources (OIR) in providing Year 2000 remediation support services.

SCOPE AND METHODOLOGY

Division of State Audit staff reviewed the State of Tennessee's remediation efforts for the Year 2000 based on representations by appropriate staff in state agencies and institutions of higher education. Work commenced on the review in August 1998 and concluded in April 1999. Because of the number of respondents and the timing of their responses, the information was received throughout the review period. Information collected from respondents during the earlier

part of the review period may not accurately reflect their conditions during the latter part of the review period because of the progress they may have achieved during the elapsed months.

The review was performed using surveys, questionnaires, interviews, and reviews of information provided by the Year 2000 Project Manager, Year 2000 Coordinators, and other appropriate staff in state agencies and institutions of higher education. Review efforts focused on the remediation status of mission-critical application systems because of their pervasive effect on government operations. Auditors initially administered surveys to, and completed standardized questionnaires with, Year 2000 Coordinators and other appropriate staff in 53 state agencies, 20 Tennessee Board of Regents institutions, and seven University of Tennessee institutions between August and October 1998. This effort provided an inventory and the status of remediation for mission-critical application systems and infrastructure components of computer systems as reported by individual Year 2000 Coordinators. Once compiled, this information was provided to the state's Year 2000 Project Manager and Year 2000 Coordinators of the University of Tennessee and the Tennessee Board of Regents in order to corroborate or to supplement their information. Recognizing testing of converted or replaced systems as an essential element of remediation efforts, auditors again questioned Year 2000 Coordinators and other appropriate staff in April 1999 regarding the status of testing for mission-critical applications. The review focused on state agencies and institutions of higher education. No procedures were performed pertaining to the Year 2000 efforts and activities of the federal or local governments or of private-sector third parties. The review also included

1. review of General Accounting Office (GAO) guidance for Year 2000 remediation efforts;

2. review of guidance for Year 2000 remediation efforts provided by the state's Year 2000 Project Manager on the state's website (http://www.state.tn.us/finance/oir/y2k/webindex.html); and

3. review of relevant performance audit reports on Year 2000 remediation efforts from other states.

To facilitate understanding of Year 2000 issues, the scope of this review, and relevant professional guidance, the following should be noted:

1. Division of State Audit staff did not perform any test work relating to the effectiveness of Year 2000 remediation efforts. "Remediation" as defined by GAO is the process of awareness, assessment, renovation, validation, and implementation performed to prepare systems for the Year 2000. Division staff relied on representations by appropriate staff and review of associated documentation, where available.

2. The Governmental Accounting Standards Board (GASB) in October 1998 issued Technical Bulletin 98-1, *Disclosures about Year 2000 Issues,* effective for financial statements on which the auditor's report is dated after October 31, 1998. Technical Bulletin 98-1 requires state and local governments to disclose a general description of the Year 2000 issue as it relates to their organization, including a description of the

stages of work in process or completed to make computer systems and other electronic equipment critical to conducting operations Year 2000 compliant.

3. The Audit Issues Task Force of the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) raised concerns that the disclosures for financial-statement audits required by GASB Technical Bulletin 98-1 were neither assertable by management nor verifiable by auditors. The AICPA advised auditors to be very cautious about being associated with these disclosures. According to the AICPA, "because of the unprecedented nature of the Year 2000 issue, its effects and the success of related remediation efforts will not be fully determinable until the Year 2000 and thereafter." The AICPA further stated that "accordingly, sufficient audit evidence may not exist to support the required technical bulletin disclosures." Therefore, the AICPA cautioned that auditors may need to consider issuing qualified opinions (scope limitations) with respect to such disclosures in financial-statement audits.

4. The 1998 State of Tennessee Comprehensive Annual Financial Report's Independent Auditor's Report, dated January 25, 1999, included the following statement:

> The Governmental Accounting Standards Board Technical Bulletin 98-1, *Disclosures about Year 2000 Issues,* requires disclosure of certain matters regarding the year 2000 issue . . . . Because of the unprecedented nature of the year 2000 issue, its effects and the successes of related remediation efforts will not be fully determinable until the year 2000 and thereafter. Accordingly, insufficient audit evidence exists to support the State of Tennessee's disclosures with respect to the year 2000. . . . Further, we do not provide assurance that the State of Tennessee is or will be year 2000 ready, that the State of Tennessee's year 2000 remediation efforts will be successful in whole or in part, or that the parties with which the State of Tennessee does business will be year 2000 ready.

Despite reasonable and diligent efforts by state officials, the ultimate effectiveness of Year 2000 remediation efforts cannot be determined with complete assurance until January 1, 2000.

BACKGROUND INFORMATION

THE YEAR 2000 PROBLEM

According to the United States General Accounting Office,

> The Year 2000 problem is rooted in the way dates are recorded and computed in many computer systems. For the past several decades, systems have typically used two digits to represent the year, such as "97" representing 1997, in order to conserve on electronic data storage and reduce operating costs. With this two-digit format, however, the Year 2000 is indistinguishable from 1900, 2001 from 1901, and so on. As a result of this ambiguity, system or application programs that use dates to perform calculations, comparisons, or sorting may generate incorrect results when working with years after 1999.

The Year 2000 problem pertains not only to application systems (computer programs that provide fiscal and administrative services), but also to other software systems, hardware, telecommunications systems, and embedded systems. Embedded systems are microprocessors (computer chips) found in a vast array of devices, such as biomedical equipment used at health care facilities, electrical monitoring and distribution devices used by utility companies, communication systems, building security and fire systems, elevators, traffic control and street light systems, automated heating and cooling systems, and even basic office equipment.

STATE OF TENNESSEE'S YEAR 2000 EFFORTS

State Agencies

According to the Year 2000 Status Report dated April 1, 1999, posted on the state's Year 2000 web page, the Office for Information Resources (OIR) in the Department of Finance and Administration estimates the total costs to the State of Tennessee for Year 2000 conversion to be $15,640,417, including both state and federal funds. To address Year 2000 issues, the General Assembly appropriated $6 million for fiscal year 1998 and another $4 million for fiscal year 1999 to the Systems Development Fund administered by OIR. Based on unaudited information from the State of Tennessee Accounting and Reporting System, $6,224,969 (62%) of these appropriations had been expended as of January 31, 1999. The percentage of total estimated expenditures as of February 1, 1999, was a similar 63% ($9,920,983) according to unaudited information from OIR. This reported expenditure includes appropriated state dollars as well as charges to federal programs. In addition, agency Year 2000 Coordinators informed audit staff that Year 2000 efforts were also being funded through agencies' existing budgets. However,

because agencies did not specifically classify these costs as Year 2000 costs, we were unable to accumulate total state Year 2000 expenditures.

OIR's responsibilities are broad and diverse. According to the *1998-99 State of Tennessee Information Systems Plan*, OIR provides direction, planning, resources, and coordination in managing the information technology needs of the State of Tennessee. OIR's clients and partners consist of state agencies, departments, commissions, local education agencies, K-12 schools, and higher education.

The environment of the state's government information systems appears to operate in essentially a two-tier structure. One tier includes centralized systems administered by the respective state agencies but supported by OIR and processed on the state's mainframe computer. The second tier includes internal agency systems both administered and supported by agency staff.

Operating as a multi-purpose computer service bureau, OIR provides agency clients a centralized data center including mainframe computer processing, data management, and telecommunications services. The majority of the critical financial management and program administration application systems crucial to the operations of state government reside and are processed at OIR's data center in Nashville. In addition, OIR's Office of Systems Development and Support provides computer programming services including Year 2000 remediation for the majority of the centralized applications. However, regardless of the extent of support services provided by OIR, the ultimate responsibility for the effectiveness of agency computer systems resides with the owner agency.

The respective agencies' mid-level or local area network (LAN) systems provide the supporting computer system infrastructure upon which the internal agency application systems reside and are processed. Some state agencies have information systems staff on site who perform programming and operations services in support of their systems.

In April 1996, OIR established a Year 2000 Project Manager position. Other than the project manager, no additional staff have been directly assigned to this function. It should be noted that the project manager does not directly supervise staff responsible for Year 2000 changes. Intrinsic to the structure of the function of Year 2000 Project Manager is that his office has the responsibility for issuing guidelines and for requiring compliance by executive branch agency staff. However, the manager has no explicit authority for requiring compliance by nonexecutive branch state agency staff, including institutions of higher education.

According to the project manager, the efforts of OIR and the state agencies have focused on the following:

1. Developing an inventory of all production application systems residing on the state's various computer platforms (mainframe, mid-level, and micro).

2. Identifying application systems that were not Year 2000 compliant and therefore needed remediation.

3. Selecting and implementing a tool for estimating the extent of the Year 2000 problem existing in mainframe applications.

4. Assessing the impact of the noncompliant application systems on the agencies that use them, culminating in the prioritization of these systems into fatal, critical, manageable, or marginal categories. (See Exhibit, page 7).

5. Developing cost estimates for the state's Year 2000 renovation efforts relative to mainframe, mid-level, and microcomputer systems (including hardware, software, and embedded systems) based on information provided by state agencies and OIR staff.

6. Remediating application systems through the life cycle of code/database repair and testing, acceptance testing, compliance certification, and movement to the production environment; other ongoing remediation efforts include telecommunications hardware and software, operating system software across all the state's technical architecture, and hardware remediation or replacement across all the state's technical architecture.

7. Selecting and distributing Y2KPCPro, a software solution to correct microcomputer Year 2000 hardware deficiencies.

8. Soliciting from state agencies a listing of interfaces between the agencies' systems and systems external to the agency.

9. Establishing a Year 2000 Coordinators Group comprising coordinators from 53 agencies who are the focal points for all agency awareness, remediation, and compliance certification for Year 2000 related issues.

10. Conducting various awareness meetings and educational seminars for a variety of public and private groups and creating and maintaining the state's Year 2000 website as a tool for the dissemination of information and the status of the state's Year 2000 efforts.

11. Compiling monthly the status of work efforts relating to Year 2000 remediation, including OIR self-reported expenditures and agency self-reported expenditures.

12. Providing the service of the Year 2000 Project Manager as the state's contact person for requests for information about the state's Year 2000 efforts and other Year 2000 issues.

Exhibit

BUSINESS IMPACT RISK ANALYSIS CATEGORIES

Fatal:	Agency or governmental entity will be unable to complete required legal obligations or business functions if the application fails to operate. Many people would be affected, either inside and/or outside the organization. Potential liability is a possibility.
Critical:	Application will continue to operate partially; some calculations will produce incorrect results. Workarounds are short-term and highly invasive until the problem is resolved.
Manageable:	Application will continue to operate partially and/or some calculations will produce incorrect results. However, workarounds are less invasive and could be sustained for a longer period of time.
Marginal:	Minor inconvenience, annoyance, or irritation. Business will continue to function.

Source: State of Tennessee Year 2000 website, August 11, 1998.

University of Tennessee

According to the Year 2000 Coordinator for the University of Tennessee's University-Wide Administration (UWA), the UWA is responsible for ensuring the Year 2000 remediation of UT's centralized administrative systems. These systems include the university's core business-related systems, such as general ledger, procurement, accounts payable, human resources, and budget systems. All member institutions of the university system rely on these centralized systems for essential administrative services. Member institutions operate essentially as autonomous units in regard to their administration of subsidiary computer information systems and other equipment. As a result of this structure, UT's UWA has been responsible for ensuring that the centralized administrative systems are Year 2000 ready. However, individual institutions are responsible for ensuring that their subsidiary computer information systems and other equipment are Year 2000 ready.

Tennessee Board of Regents

According to the Year 2000 Coordinator for the Tennessee Board of Regents (TBR), its Office of Information Technologies (OIT) plays a major role in supporting institutions through its support of the administrative software applications. All member institutions of the TBR system utilize the same application systems for essential administrative services—the Financial Records System (FRS), the Human Resource System (HRS), and the Student Information System (SIS).

These applications are provided under a maintenance agreement with Systems & Computer Technology Corporation (SCT), headquartered in Malvern, Pennsylvania. OIT serves as the central point of contact between the vendor and the institutions. OIT relies on the vendor to provide Year 2000 ready baseline application systems which OIT then modifies specifically for Tennessee higher education before distribution to the institutions. These modifications are not Year 2000 related. However, OIT tests its modifications and the overall operational functioning of the respective systems including Year 2000 readiness. OIT distributes modified systems and implementation instructions to the institutions and requires the individual institutions to test the applications in their environment to the extent they deem necessary prior to final implementation.

Thus, the responsibility for developing baseline Year 2000 compliant systems rests with SCT, while the responsibility for performing modifications, testing system effectiveness, and installing SCT systems rests with OIT and each institution's information systems staff. Member institutions are responsible for making minor modifications specific to their operations and for testing program modifications within their facilities. Member institutions operate essentially as autonomous units in regard to their administration of subsidiary computer information systems and other equipment. However, individual institutions are responsible for ensuring that their subsidiary computer information systems and other equipment are Year 2000 ready and that approved modifications are implemented on a timely basis.

REVIEW METHODOLOGY

The review was performed using surveys, interviews, and reviews of information provided by the Year 2000 Project Manager, Year 2000 Coordinators, and other appropriate staff in state agencies and institutions of higher education. The objectives of the survey were to develop a comprehensive inventory of application systems and supporting infrastructure components of computer systems (supporting software systems, hardware, and communications equipment) from state agencies and institutions of higher education; to determine the degree of remediation of mission-critical systems; and to obtain from state agencies assessments of the performance of the Office for Information Resources, Department of Finance and Administration. For all categories of at-risk hardware or software components except interfaces, respondents were asked to provide information regarding the following:

- Projected Year 2000 impact
- Update action
- Percent Year 2000 ready as of the date of the survey
- Year 2000 certifications
- Testing
- Documentation of test results

For interfaces, respondents were asked to provide information regarding the following:

- Names of interfacing systems
- Direction of the interface

- Owner of the interfacing system
- Year 2000 readiness of the interfacing system

In August and September 1998, auditors sent surveys to 58 officials in 53 state agencies and 27 officials in 27 institutions of higher education. All state agencies and institutions of higher education have returned their completed survey forms.

Using a standardized questionnaire, auditors interviewed Year 2000 Coordinators and other appropriate staff in 53 state agencies, 20 Tennessee Board of Regents institutions, and seven University of Tennessee facilities between August and October 1998. Because of the operational structure of the University of Tennessee at Knoxville, separate questionnaires were administered for the University of Tennessee at Knoxville campus, the University-Wide Administration, and the University of Tennessee at Knoxville Medical Center, in addition to the four satellite campuses. The questionnaire was designed to obtain general responses on each entity's actions in the following areas:

- Strategy documentation
- Project plan development
- Management support
- Schedule adherence
- Impact analyses
- Comparison to similar entities
- Cost estimates
- Assessment of legal liability
- Inventorying
- Testing
- Certifications
- Data exchanges
- Test plans
- Business continuity planning

The results of the surveys and questionnaires were provided to the appropriate staff in the Office for Information Resources, the University of Tennessee, and the Tennessee Board of Regents in December 1998 and January 1999.

Auditors interviewed the Year 2000 Project Manager prior to distributing the surveys and during fieldwork. Auditors also obtained and reviewed supporting documentation from the Year 2000 Project Manager, Year 2000 Coordinators, and other appropriate staff in state agencies and institutions of higher education.

ANALYSIS AND EVALUATION

Inventories of Mission-Critical Application Systems and Infrastructure Components of Computer Systems Have Been Developed

The state's Year 2000 Project Manager has developed an inventory of mission-critical application systems. According to the project manager, he began his monitoring effort in October 1996 focusing on unremediated mainframe and mid-level application systems. He later expanded his monitoring system in December 1997 to include PC application systems, hardware, other software, and telecommunications as reported on agency work plans. However, the primary focus remained on the unremediated centralized systems. In March 1998, he developed a list of the state's mission-critical application systems for use in a Securities and Exchange Commission (SEC) disclosure statement accompanying a bond issuance. The SEC list consisted of those unremediated centralized application systems the agencies had identified as either fatal or critical. That early mission-critical list totaled 156 systems. He explained that a few of those systems were later identified as obsolete or reclassified by their owner agencies as manageable or marginal. Therefore, he revised the number downward from 156 to 148 in November 1998.

In August and September 1998, the Division of State Audit surveyed state agencies asking them to rank their systems according to the State of Tennessee Year 2000 Project Manager's classification system (fatal, critical, manageable, or marginal). To assist agencies, audit staff used the project manager's list of mainframe and mid-level systems and the PC applications from the agency work plans. Agencies were then asked to list any additional systems they administered, regardless of the system's need for remediation. Therefore, the resulting list of systems identified as fatal or critical was larger than the mission-critical list prepared by the project manager. The project manager's list of 148 systems did not include PC application systems or systems deemed compliant by the agencies.

In December 1998, the project manager then broadened his list of mission-critical systems to include PC mission-critical application systems. In addition, he added systems that had been identified in our survey but not included previously in his list. The result was a mission-critical list of 326 systems.

The auditors' survey resulted in a list of 269 mission-critical application systems. Of those, 39 items were determined to be erroneously classified as application systems. Therefore, the actual population of mission-critical application systems reported to the Division of State Audit totaled 230. All but 39 of the remaining 230 (i.e., 191) application systems appear on the project manager's mission-critical list. The reason these 39 systems were not included is that the agencies reported them to the project manager as less than mission critical on their monthly work plans, and the project manager regarded the work plan data as more current than the survey data. The project manager's list also included 135 application systems not identified as mission critical on the survey. Although not reported as mission critical on the survey, these systems were

categorized on the monthly work plans as mission critical. Again, the project manager regarded that information as more current than the survey data.

There were three limitations in comparing survey results to data from the OIR project manager:

1. There were differences in the way percentages of remediation data were reported to the Division of State Audit in the survey results and the way the data were reported to OIR. Agencies reported total estimated hours of effort, expended hours, and remaining hours to OIR; survey respondents were asked to provide their best estimate of the system's percentage of remediation toward Year 2000 readiness. As a result, the project manager had data to calculate the percentage remediated, but no overall percentage remediated could be determined from survey responses.

2. Survey responses were self-reported data from the agencies.

3. Survey responses were received from August 1998 through January 1999 and are therefore not concurrent with the data from the Year 2000 Project Manager.

The University of Tennessee and the Tennessee Board of Regents have each identified mission-critical application systems (also identified as "essential administrative systems") used by all campuses of the respective systems. In addition, the Year 2000 Project Manager and the Year 2000 Coordinators of the University of Tennessee and the Tennessee Board of Regents have compiled inventories of infrastructure components of computer systems.

Remediation Efforts for Mission-Critical Application Systems and Infrastructure Components of Computer Systems Are in Progress

Mission-Critical Application Systems

Auditors have observed evidence of remediation efforts throughout the review period. Remediation efforts are in progress for state agencies and institutions of higher education and are expected to continue through the end of the current calendar year. Overall, as of January 19, 1999, the Year 2000 Project Manager reported 90% remediation for state agency mission-critical systems, 87% remediation for University of Tennessee essential administrative systems, and 90% remediation for Tennessee Board of Regents essential administrative systems. The extent of completion of total remediation efforts noted above is based on percentage of total work effort planned, including testing. The bases for these percentages are discussed below.

<u>90% Remediation for State Agency Mission-Critical Application Systems</u>

Mission-critical systems are those application systems classified by their owner agencies as either fatal or critical. Owner agencies classified 326 systems as mission critical. (See Exhibit,

page 7, for a description of these categories.) Progress for remediating systems is measured in remaining hours needed to complete remediation against total estimated hours. Specifically, the project manager stated that he divided remaining hours by total estimated hours, then subtracted the result from 1. For example, if the total estimated hours were 100, and the remaining hours were 10, the project manager would divide 10 by 100, resulting in 0.1, then subtract 0.1 from 1.0, resulting in 0.9, otherwise stated as 90% remediated.

According to the project manager, total estimated hours were developed by one of two methods. The first method involved a complex process of analysis and professional judgment for centralized OIR-supported systems as described on the state's Year 2000 website (http://www.state.tn.us/finance/oir/Y2K/estforms.html). A second method relied on agency representations of the hours required for internal agency-supported systems.

On January 19, 1999, the Year 2000 Project Manager updated the Information Systems Council, stating that work on all state agency mission-critical application systems was 90% remediated. The council is the state's executive steering committee presiding over the state's information systems community. Council membership consists of the following:

- Commissioner of Finance and Administration (the chair)
- Commissioner of General Services
- Comptroller of the Treasury
- Three members of the Senate
- Three members of the House of Representatives
- Two private citizens who have demonstrated expertise and experience in managing large and diverse information management systems
- One member of the Tennessee Regulatory Authority
- Two non-voting members—the chair of the Information Systems Management group and a state employee selected by the Tennessee State Employees Association who has experience in the field of information systems
- The Chief Justice of the Supreme Court of Tennessee or designee

Division of State Audit staff obtained work plan data from the project manager showing the total estimated and remaining hours by system and analyzed the percentage remediated for each system. The state's mission-critical production application systems were distinguished as to whether they were

- certified as Year 2000 compliant by the owner agencies (54 application systems),
- remediated, but no certification on file (106 application systems),
- scheduled to be replaced (63 application systems),
- scheduled for remediation by vendor (13 application systems),
- obsolete (3 application systems), or
- remediation in progress (88 application systems).

These categories add to 327, one more than the project manager's mission-critical list of 326, because the Tax Relief system is reported on the project manager's list as one system, but

the system is shown on the work plan in two parts—one part is certified, and the other is still in process of remediation.

The percentages should be understood in the context of the following five qualifications. First, for systems that were certified or remediated but not certified as of December 1997, agencies were not required to report the estimated hours necessary to make those systems Year 2000 ready or the hours actually expended. Second, estimated and actual hours are not reported for obsolete systems because these systems will be discarded. Third, estimated and actual hours are not reported for replacement systems because those systems will be superceded by systems expected to be Year 2000 ready. Because these projected replacement systems have not been remediated and tested, the extent of their Year 2000 compliance cannot be feasibly estimated, nor can the level of effort to ensure Year 2000 compliance be determined. Fourth, systems to be remediated by vendors also do not show estimated and actual hours because the vendors have not been required to report estimated and actual hours. According to OIR, the contract language requires systems remediated by vendors to be Year 2000 compliant. Therefore, in the event a vendor-remediated system fails to be Year 2000 compliant, the failure would become a contract performance issue. Finally, the information for some systems reported in the work plan as under remediation was not sufficient to calculate the percentage of remediation. Therefore, the overall remediation percentage is based only on those systems for which reported hours are available (180 systems).

Based on the hours provided, audit staff calculated the percentage remediated for the mission-critical application systems at 91%. The difference between the auditors' calculation of 91% and the project manager's of 90% is not material and appears to be the result of rounding. The project manager's calculations divide the estimated remaining hours to remediate by the original estimated hours and subtract the result from 1.0, even though for some systems the sum of actual hours expended plus estimated remaining hours needed to remediate exceed the original estimated hours. Auditors recalculated the percentage remediation using adjusted hours (the sum of hours to date and the estimated remaining hours needed to remediate) as the base.

As an illustration, assume that the original estimated hours are 1,000, the hours to date were originally 900, and the estimated remaining hours are 500. Using the project manager's method, the remediation percentage would be 50% (1 – (500/1,000) = 0.5 or 50%). However, this percentage would be incorrect if the base number has changed from 1,000 to 1,400 (900 + 500). Therefore, the correct remediation percentage would be 64% (1 – (500/1,400) = 0.64 or 64%). Auditors recalculated the overall remediation rate using the second formula. The difference between the project manager's method and the auditor's method of calculation is not material because the results varied by one percent.

Audit staff compared the percentage remediation as shown on the project manager's work plan dated January 1999 to the percentage remediation agencies reported on their survey forms from September 1998 for each mission-critical system. The 327 systems compared as follows:

- 78 (24%) showed a match between the survey responses and the project manager's work plan.

- 66 (20%) showed the work plan percentage higher than the survey response.

- 122 (37%) showed that the system was remediated, would be replaced, or would be remediated by a vendor, so no hours were required on the project manager's work plan. Without reported hours, a percentage remediated could not be calculated or compared.

- 37 (11%) showed no percentage remediated on the work plan for systems under remediation; therefore, no comparison could be made. Lack of data indicates the need for project manager review.

- 24 (7%) showed the survey response percentage higher than the work plan, indicating the need for project manager review. A copy of the list of discrepancies was provided to the project manager for his review on February 26, 1999.

87% Remediation for University of Tennessee Essential Administrative Systems

The University of Tennessee's University-Wide Administration (UWA) calculates an estimated Year 2000 percentage of remediation monthly for the essential administrative systems. This estimated percentage is calculated by dividing remediation hours expended to date by the sum of remediation hours expended to date and estimated remaining hours to remediate. The UWA Year 2000 Coordinator provides the percentage monthly to OIR's Year 2000 Project Manager for monitoring and reporting to the Information Systems Council. As of January 19, 1999, UWA's Year 2000 Coordinator reported an estimated 87% remediation for essential administrative systems.

90% Remediation for Tennessee Board of Regents Essential Administrative Systems

Member institutions and the board's Office of Information Technology (OIT) prepare an estimated Year 2000 percentage of remediation monthly for the three essential administrative systems. These estimated percentages are summed and divided by 21 (20 member institutions and the OIT) and reported by the OIT to OIR's Year 2000 Project Manager for monitoring and reporting to the Information Systems Council. As of January 19, 1999, OIT reported an estimated 90% remediation for essential administrative systems.

The board's current maintenance agreement with Systems & Computer Technology Corporation (SCT) does not specifically identify Year 2000 readiness as an obligation of the vendor. However, on November 25, 1998, SCT issued its customers a Year 2000 Readiness Disclosure wherein it stated:

> SCT has been in the process of updating all of the systems that are part of the Plus2000 product line to support the year 2000 since 1991 when SIS/FAM version 1.0 was released. We have modified the other Plus2000 products and performed tests on all of the products since then and have found some issues as a result of these tests and have corrected them in several products and are in the process of correcting them in other products. Based on these tests,

> SCT believes that the products set forth below, when used in accordance with their applicable documentation in an isolated environment, are designed to address the Year 2000. To be up to date and ready to support the year 2000, all products must be kept current as maintenance bulletins are released. . . .
>
> | PRODUCT | RELEASE |
> |---|---|
> | Financial Record System (FRS) | 3.0 |
> | Human Resource System (HRS) | 4.1 |
> | Student Information System (SIS) | 1.17 |

According to OIT, board institutions are using FRS version 3.0 and SIS version 1.17, the most current product releases. The estimated 10 percent remaining effort relates to the institutions' efforts to upgrade HRS from version 4.0 to 4.1. OIT's planned completion date for full implementation of HRS version 4.1 is no later than June 1, 1999.

Testing of Mission-Critical Application Systems

Testing is the final phase in the remediation process. The Office for Information Resources (OIR) and the statewide Year 2000 Project Manager had established December 31, 1998, as the target date for renovating mission-critical application systems, so that calendar year 1999 could be used for testing. In April 1999, division staff contacted the Year 2000 Coordinators for each agency reporting mission-critical application systems to determine the current status of testing for those systems.

Of the combined 334 mission-critical application systems reported by state agencies and institutions of higher education, testing was either complete or in progress for 90 percent of state agency systems, 100 percent of University of Tennessee systems, and 100 percent of Tennessee Board of Regents systems. The expected completion dates for systems currently undergoing testing ranged from April to October 1999. These percentages vary from those noted for total remediation since these figures (1) are on a per-system basis, (2) reflect conditions after the total remediation percentages were obtained, and (3) are limited to the testing phase of remediation. For the 30 remaining state agency systems, testing was planned for 18, and expected completion dates ranged from May to September 1999. Coordinators also reported 12 systems (4 percent of the total 334 mission-critical systems) for which no testing was planned. Coordinators cited the following reasons for not testing these systems: the systems are no longer used or will not be used as of January 1, 2000, or the systems do not process date fields.

Infrastructure Components of Computer Systems

In addition to obtaining an inventory of infrastructure components of computer systems, the auditors' survey was designed to obtain reported remediation status for these components. The results of the survey indicated that overall for the 611 mission-critical hardware items, 365 (60%) were 100% remediated, for 58 (9%) there was some progress, while for 188 (31%) there was no measurable progress. For the 470 mission-critical other software items, 243 (52%) were

100% remediated, for 89 (19%) there was some progress, while for 138 (29%) there was no measurable progress. For the 76 mission-critical communications items, 29 (38%) were 100% remediated, for 14 (18%) there was some progress, while for 33 (43%) there was no measurable progress.

As previously noted, information obtained through the auditors' survey and questionnaires relating to infrastructure components of computer systems was provided to the state's Year 2000 Project Manager and Year 2000 Coordinators of the University of Tennessee and the Tennessee Board of Regents in order to corroborate or supplement their information. Remediation efforts are continuing for these components.

State Agencies Rated the State of Tennessee's Office for Information Resources (OIR's) Year 2000 Support Activities as Excellent or Good

The Year 2000 Project Manager asked state agencies to inventory their internal applications and determine what was needed to make those systems Year 2000 ready. OIR made information and resources available for agencies to use in making these determinations and evaluating their needs. This information has been provided on OIR's website and by personal and telephone contacts.

Fifty-three state agencies were surveyed. Of the state agencies that responded to the survey and rated OIR's performance, most assessed OIR's Year 2000 support as excellent or good in the following categories:

Problem Awareness	22 of 34 respondents (65%) rated support as excellent and 11 (32%) rated support as good, for a total of 97%.
Problem Assessment	14 of 34 respondents (41%) rated support as excellent and 15 (44%) rated support as good, for a total of 85%.
Technical Assistance	14 of 34 respondents (41%) rated support as excellent and 16 (47%) rated support as good, for a total of 88%.
Program Modifications	10 of 24 respondents (42%) rated support as excellent and 11 (46%) rated support as good, for a total of 88%.
Program Testing	8 of 21 respondents (38%) rated support as excellent and 10 (48%) rated support as good, for a total of 86%.
Revision Implementation	7 of 21 respondents (33%) rated support as excellent and 10 (48%) rated support as good, for a total of 81%.
Funding Assistance	5 of 19 respondents (26%) rated support as excellent and 7 (37%) rated support as good, for a total of 63%.

The only poor responses received were one (3%) for Technical Assistance and three (16%) for Funding Assistance.

A readily available source of technical support is of paramount importance to the agencies as they identify and correct their particular variations of the Year 2000 problem. These responses indicate that OIR has taken direct and positive action to meet this need.

Mission-Critical Application Systems Reported as Remediated by Programming Staff Were Not Always Certified as Remediated by Owners

A review of the 327 mission-critical application systems identified 106 systems that their respective agencies had reported as completely remediated, but for which the project manager had not received duly completed certificates of compliance from the owner agencies. Overall, as of January 28, 1999, the agencies had reported 160 remediated systems, of which 54 had been duly certified.

Each agency is to ensure that remediated systems meet the certification standards established by the State of Tennessee's Office for Information Resources (OIR). Additionally, OIR has stated that after remediation is complete, the respective agency is responsible for certifying to OIR that the system is Year 2000 compliant. OIR has established a list of standards that define "Year 2000 compliance" for the State of Tennessee. These standards can be found on OIR's web page at http://www.state.tn.us/finance/oir/y2k/standard.html. To assist in certification, OIR has made a standard compliance form available to the agencies at http://www.state.tn.us/finance/oir/y2k/formstat.html#com. Because the owner agency is responsible for accepting a system's remediation and ensuring that the system meets the standards, OIR relies on the information the individual agencies provide. OIR does not independently certify any system as Year 2000 compliant, except for those systems it directly owns.

OIR's receipt of these signed certifications of compliance is important because the certifications provide OIR with the owner agency's formal sign-off, indicating (1) the application meets OIR's standards for compliance and (2) the appropriate staff in the owner agency accept the final product. In addition, the project manager publicly reports the number of compliance statements received as a benchmark of remediation efforts. Therefore, prompt receipt of properly signed and completed certifications of compliance provides the basis for accurate reporting.

Recommendation:

OIR should emphasize the importance of submitting certifications of compliance when agency systems meet the standards. In addition, OIR should promptly reject certifications containing alterations to the standard wording. For example, one agency submitted a certification

form on September 26, 1996, but noted on the form, "vendor is modifying software at this time—will be compliant by 7-1-97." The note clearly indicates that the certification was inappropriate because the remediation process had yet to be completed. Auditors found 9 certification forms that were similarly defective. The count of 54 completed certification forms cited above includes only unaltered forms.

Management's Comment:

Department of Finance and Administration

We concur. The process that OIR has followed has not placed great emphasis on the certification letter early in the process because many of the departments were still involved in testing to ensure they were compliant. This testing includes outside partners which at times require more time to pursue than validating the systems works internally. Our plans have and do call for certification letters to be on file showing the systems are Year 2000 operational.

Few Entities Reported That They Had Documented Communications Regarding Interfaces Between Systems

Of the 80 entities responding to the division's interview questions, 64 entities reported having interfaces. Of those, 53 (83%) reported that they did not have written agreements with their business partners to ensure Year 2000 data compatibility:

- 34 (64%) of 53 state agencies
- 19 (95%) of 20 Tennessee Board of Regents institutions.

"Agreements" in this context means documentation of the agreed-upon format for how shared data is to be transmitted and received to ensure Year 2000 data compatibility.

The Division of State Audit survey identified 768 interfaces: 370 at state agencies (of which 217, or 59%, were reported as Year 2000 ready), 127 at University of Tennessee institutions (of which 80, or 63%, were reported as Year 2000 ready), and 271 at Tennessee Board of Regents institutions (of which 170, or 63%, were reported as Year 2000 ready).

Interfaces, also known as electronic data exchanges, transfer data between two or more business partners using electronic media (e.g., transfers from one computer to another using a dedicated network, exchanges over commercially available networks or the Internet, or exchanges of magnetic media such as tapes or disks). Interfaces occur between federal agencies, other state entities, local governments, or private-sector organizations. For interfaces to function properly during and after the Year 2000, each party to the transfer must be able to send and receive data in the appropriate format.

Formal communication regarding interfaces is important because not all organizations are addressing Year 2000 issues in the same way. Some entities are using windowing, i.e., including logic in their systems to determine that a two-digit year is preceded by a 19 or a 20 based on whether the year is before or after a given year. For example, when the two-digit year is 50 or above, the system assigns the century as 19, i.e., 1950; whereas when the two-digit year is 49 or below, the system assigns the century as 20, i.e., 2049. This example is one of several windowing alternative solutions. Other organizations are designing their systems to read only four-digit year fields. If each party to an interface uses a different method, the data may be incompatible and may not be transferred or may not be transferred effectively.

OIR's standard for interfaces for state agencies is a four-digit year field. OIR guidance states that if existing systems cannot comply with the standard and yet must interface with other systems, both entities must agree, in writing, to the date format represented in the application. The guidance further states that both parties should keep a copy of this agreement.

According to University of Tennessee officials, the University-Wide Administration (UWA) promulgates data exchange standards for all intercampus interfaces; thus, according to UT officials, interfaces are well documented. UWA generally uses a two-digit year format in conjunction with "windowing" programming techniques to achieve data exchanges. UWA has reportedly documented these requirements along with data exchange requirements with external financial institutions and the state and federal governments.

The Tennessee Board of Regents does not utilize a standard format for date fields.

Although the absence of written agreements does not mean that agency staff have not considered appropriate date formats to enable interfacing, formal documentation of such determinations would appear appropriate. Such documentation would ensure that appropriate staff have in fact communicated with their data exchange partners and that relevant information has been shared.

Interfaces directly affect the timeliness, efficiency, and accuracy with which government operates. Interfaces effectuate the transfer of funds and information among business partners. Therefore, timely, accurate interfaces are vital to the efficient and effective functioning of state government. By not documenting their understandings related to data exchanges, entities risk miscommunication, corrupted data, and delays in transferring needed information.

Recommendation:

Management should ensure that communications regarding date formats for transmitting and receiving data are documented.

Managements' Comments:

Department of Finance and Administration

We concur. While we feel that the numbers given in the analysis are not reflective of the actual amount of work and documentation on interfaces, we concur that interface work should be documented. The state and federal government spent a significant amount of time documenting both the data and the format of the interface exchanges. The documentation of the interfaces with the business partners will happen during the testing period. OIR will reinforce the need to document these interfaces with the Year 2000 coordinators during May and June of this year.

Tennessee Board of Regents

We concur. Attempts are being made to obtain written documentation regarding date format for transmitting and receiving data. We are recommending to the institutions that they obtain like documentation from their data exchange partners.

Although Inventories of Mission-Critical Application Systems Had Been Developed, Few Entities Reported Conducting an Inventory of Embedded Systems and Performing Risk Assessments of These Systems

Embedded systems are microprocessors (computer chips) found in a vast array of devices, such as biomedical equipment used at health care facilities, electrical monitoring and distribution devices used by utility companies, communication systems, building security and fire systems, elevators, traffic control and street light systems, automated heating and cooling systems, and even basic office equipment, including computers and peripheral equipment (hardware).

Division of State Audit staff conducted interviews using a standardized questionnaire with appropriate staff in 80 entities. Twenty-nine of the 80 responded Not Applicable to the question, "Do you have an inventory of systems with embedded chips?" Seven entities responded that they had conducted an inventory, and 44 answered that they had not conducted an inventory:

- 23 (43%) of 53 state agencies
- 4 (57%) of 7 University of Tennessee institutions
- 17 (85%) of 20 Tennessee Board of Regents institutions.

On November 13, 1997, OIR instructed agencies to provide to the Year 2000 Project Manager a listing of all of their projects, including embedded systems. OIR requested that agencies provide this information by December 15, 1997, and update it each month. Agencies have provided and are updating listings of their projects as requested.

The Division of State Audit analyzed the current inventory listing submitted to the project manager as of January 19, 1999. Individual agencies are responsible for reporting on embedded systems applicable to their specific needs. Included in the work plan are responses from OIR's telecommunications section and the Department of General Services identifying embedded systems for which they are responsible. Forty-four of 80 entities questioned reported that they had not inventoried their embedded systems. An additional 29 responded that an inventory of embedded systems did not apply to them. These 29 entities were state agencies and included the Departments of Agriculture, Correction, Environment and Conservation, Health, and Mental Health and Mental Retardation. Because of the size and multifunctional nature of these departments, it is likely that they do utilize embedded systems.

Just as with application systems and infrastructure components of computer systems, each agency or institution of higher education needs a comprehensive inventory of embedded systems. These inventories would identify embedded systems falling under the authority of OIR, the Department of General Services, or the entity itself. To ensure continuation of services, entities must identify their embedded systems, determine which systems are essential through a risk assessment process, and prepare contingency plans for continuing operations in case essential embedded systems fail.

Recommendation:

Management should ensure it has prepared comprehensive inventories and performed risk assessments of embedded systems to develop effective contingency plans in case the essential embedded systems fail.

Managements' Comments:

Department of Finance and Administration

We concur in part. As the Year 2000 project has progressed and as we have learned more about the possible impact of embedded chips, the technical community has learned that the risks in this area are not as large as once thought. The percentage estimates of those that pose a problem continues to fall. The state, through its central functions in OIR and General Services, is taking care of some of the items such as communications devices, security, and HVAC. We do believe and will encourage those that have embedded chips that have been documented to pose problems to inventory and verify they are compliant or complete a contingency plan. Areas of concern include Corrections facilities and those departments that are involved with the delivery of medical services. We will begin this activity in June 1999.

University of Tennessee

We concur. However, since the Division of State Audit's interview last year, inventories of embedded systems have been performed at all University of Tennessee institutions as part of

the University's continuing Year 2000 efforts. Vendors of all equipment utilizing embedded systems have been contacted with inquiries regarding Year 2000 readiness, and responses have been received from many of them. Evaluations are continuing to be performed to determine whether replacement of essential equipment will be required.

Tennessee Board of Regents

We concur. A list of possible embedded systems, which was originally distributed by OIR, has been provided to all institutions. We have recommended to the TBR institutions that they inventory, prepare risk assessment, and document the Year 2000 compliance.

Most Entities Reported That They Had Not Established Business Continuity Plans

Of the 80 entities responding to the division's interview questions, 73 (91%) did not have business continuity plans:

- 47 (89%) of the 53 agencies
- 7 (100%) of the 7 University of Tennessee institutions
- 19 (95%) of the 20 Tennessee Board of Regents institutions.

The General Accounting Office notes in its *Year 2000 Computing Crisis: Business and Continuity Planning,*

> Despite the efforts of each business, state and local government, and federal agency to race against time and to renovate, validate, and implement their mission-critical information systems, every organization remains vulnerable to the disruption of its business processes.

Business continuity planning helps to ensure an entity maintains its critical functions in case of Year 2000-related failures of computer systems and other equipment. Business continuity planning is not an information technology issue. Continuity planning does not involve matters such as developing software "patches" for flawed systems or otherwise rewriting programs or changing system configurations. Instead, planning involves the development of operating procedures to provide continued service delivery in the event of computer system and other equipment failures. Hence, it should not be necessary to engage those technical staff addressing the Year 2000 remediation efforts in developing these plans to the extent of diverting their primary focus from the technical aspects of the Year 2000 problem.

Recommendation:

Management should establish business continuity plans to ensure the continued functioning of critical business processes. The GAO notes that a business continuity plan consists of a set of contingency plans for each core business process and infrastructure component. Each plan should provide a description of the resources, staff roles, procedures, and timetables needed for implementation.

Management should evaluate the costs and benefits of alternative operating procedures for each critical business process, selecting the one best suited for their organization. They should then define the precipitating event that would activate the plan, establish the teams to implement the plan, and define the roles and strategies to make the plan effective. The Department of Finance and Administration issued Business Resumption Planning Guidelines in August 1998. These guidelines provide a basis for focusing entity efforts in business continuity/resumption planning.

Managements' Comments:

Department of Finance and Administration

We concur. Our effort has been to focus all early attention on remediation and then focus on business planning based on the results of the remediation effort. It is a strategic direction of the Governor that the executive branches develop and test continuity plans. The plans are to be developed by June 30, 1999, and tested by September 30, 1999. OIR has encouraged all state agencies not in the Executive branch to do the same and has provided all of the Legislative and Judicial sections the same information.

University of Tennessee

We concur. The University does not have business continuity plans for those departments and offices that might be impacted by the complete loss of computing capability. The University will establish a task force to identify those offices and explore the feasibility of developing business continuity plans as part of the continuing Year 2000 readiness effort.

It must be understood, however, that a complete loss of University computing capability is considered highly unlikely barring a Year 2000 related collapse of societal infrastructure (electric power, telecommunications, etc.), in which case University services would likely be suspended pending their restoration. Short of that, should internal, short-term Year 2000-related problems arise, it is anticipated that the University's talented and resourceful staff will be able to deal with and fix each problem as it occurs.

Tennessee Board of Regents

We concur. While we have identified all critical business processes and they have been or will be made Year 2000 compliant, we also recognize that other factors beyond our control may cause failures in the computer systems and other equipment. Therefore, we are recommending that each department at TBR institutions develop a plan that would allow them to operate if such a failure occurs. The recommendation is that the department identifies whether the process is critical in the operation of the department or whether the process could be eliminated during the failure. The department would then develop the plan according to their needs.

OIR Reported Three Systems Have Potential for Major Problems in Their Remediation Efforts

As of April 1, 1999, OIR's Year 2000 Status Report stated that potential problems were being monitored as needed to ensure all mission-critical applications were successfully remediated. OIR is not directly responsible for the development or conversion of the following systems that were reported as having the potential for major problems:

- Tennessee Court Information System (TnCIS)—The State of Tennessee's Administrative Office of the Courts is developing this new system to replace several different application systems currently in use in the county courts. According to OIR staff, the new system is designed to provide uniformity in reporting and more effective statewide statistical compilation. However, TnCIS will not be implemented by December 31, 1999. Therefore, each of the systems currently in use must be made Year 2000 compliant by its respective vendor. These systems are reportedly in various stages of the remediation process, and the vendors have stated that each existing system will be ready by December 31, 1999. However, the existing systems must be remediated to ensure efficient operation of the courts.

- Tennessee Kids Information Delivery System (TNKIDS)—The Department of Children's Services is developing a new system to provide coordinated services for Tennessee's children and their families, allowing the department to track the children, their needs, and the services they receive. According to OIR, "The Department relies on several very old systems, which are not being remediated. These systems are to be replaced by the new TNKIDS system. This system must be implemented in a timely manner to provide basic business functionality." According to Department of Children's Services staff, a temporary workaround will be in place by May 3, 1999.

- TennCare Management Information System (TCMIS)—The Bureau of TennCare is remediating this system to be Year 2000 compliant with the help of Electronic Data Systems (EDS), the vendor. TCMIS tracks data relating to TennCare clients and the services they receive, as well as payments to providers. According to OIR, "The

contractor responsible for this system started remediation efforts very late and has already missed the first critical time frame. A temporary workaround is in place. Failure to complete changes to this system will result in very serious service disruptions."

Recommendation:

OIR should continue to monitor progress and provide appropriate guidance relating to these systems.

Management's Comment:

Department of Finance and Administration

We concur. OIR is continuing to monitor their progress as well as the progress of other systems. If we identify other systems that we feel move into the high-risk area, we will include them on our watch list.

APPENDIX

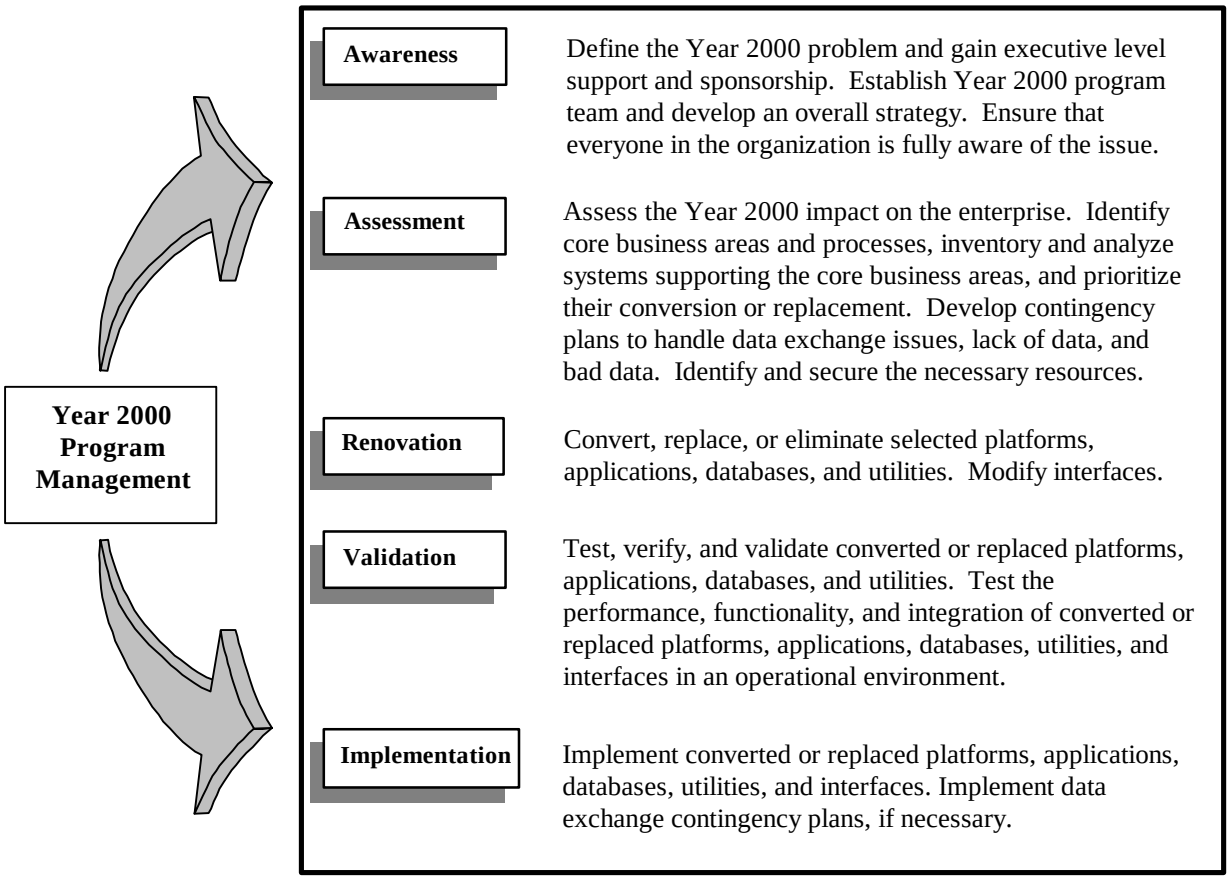
U.S. GENERAL ACCOUNTING OFFICE GUIDES

The United States General Accounting Office (GAO) has issued three published guides on Year 2000 issues as of November 30, 1998.

Year 2000 Computing Crisis: An Assessment Guide (September 1997)

In September 1997, the GAO issued *Year 2000 Computing Crisis: An Assessment Guide* as a model approach for managing Year 2000 conversion projects. The GAO model presents five stages beginning with awareness and ending with implementation. The model also defines each stage. GAO's Year 2000 assessment model presented in the guide is shown below.

GAO YEAR 2000 ASSESSMENT MODEL

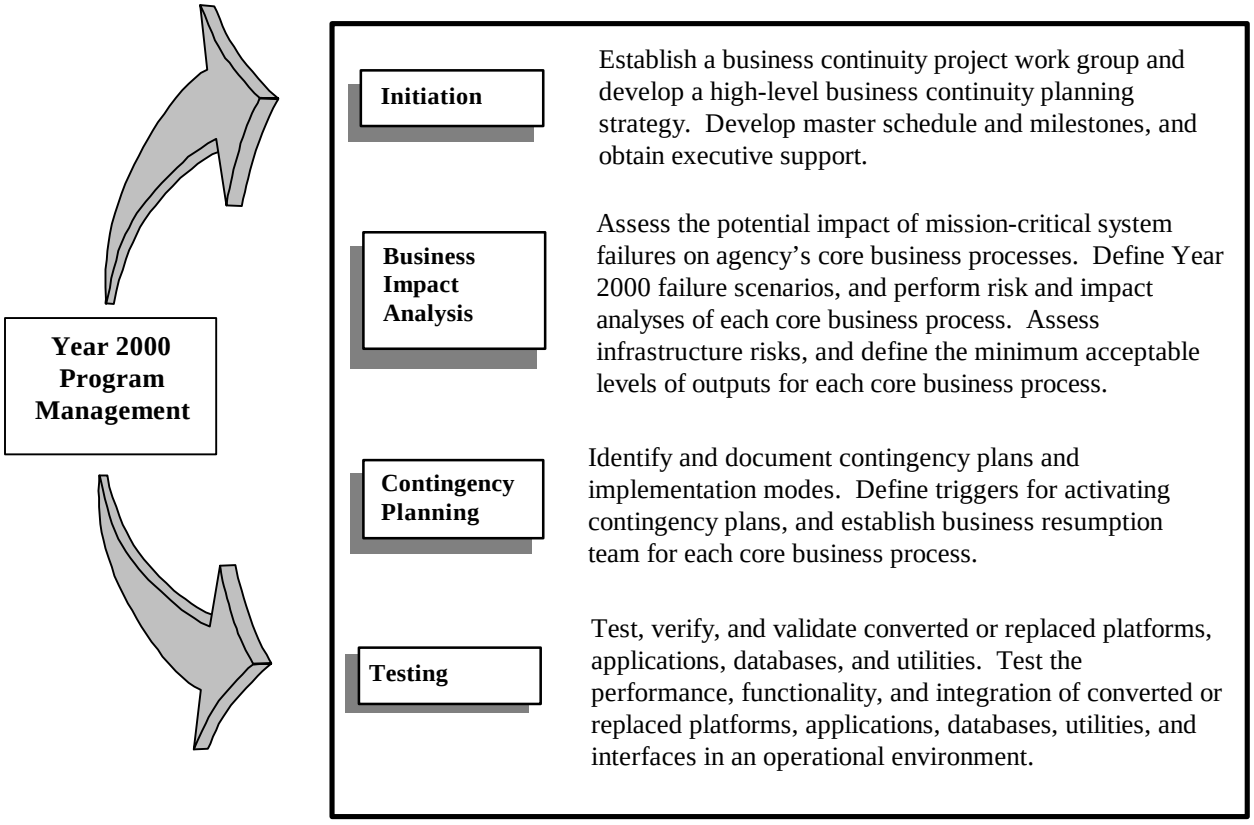


Source: *Year 2000 Computing Crisis: An Assessment Guide, September 1997.*

Year 2000 Computing Crisis: Business Continuity and Contingency Planning (August 1998)

Issued in August 1998, the GAO's publication *Year 2000 Computing Crisis: Business Continuity and Contingency Planning* provides a model for business continuity and contingency planning that focuses on the organization's core business processes. The GAO model is divided into four phases: initiation, business impact analysis, contingency planning, and testing. GAO's Year 2000 continuity planning model presented in the guide is shown below.

GAO YEAR 2000 CONTINUITY PLANNING MODEL

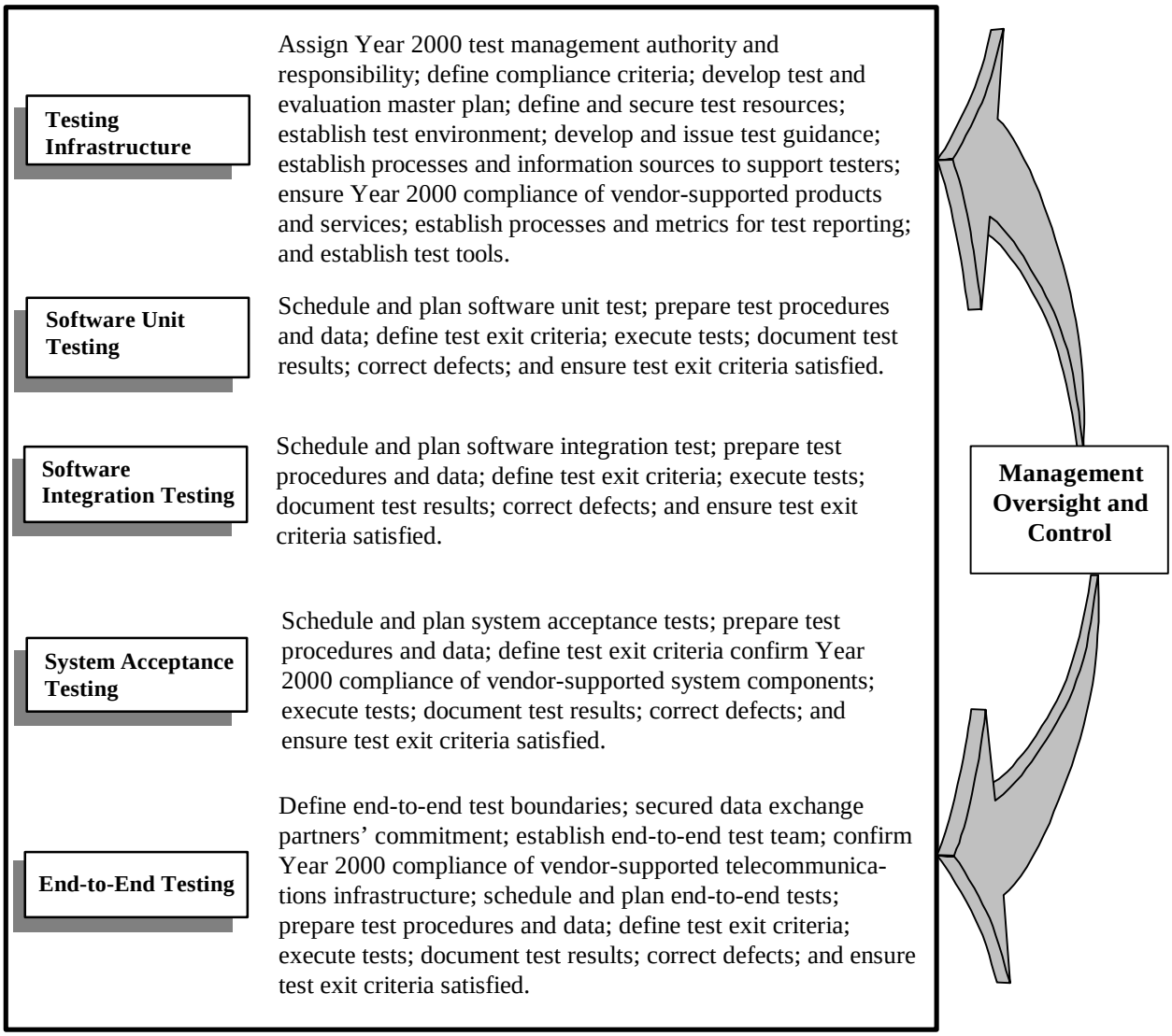


Source: *Year 2000 Computing Crisis: Business Continuity and Contingency Planning, August 1998.*

Year 2000 Computing Crisis: A Testing Guide (November 1998)

The GAO's publication *Year 2000 Computing Crisis: A Testing Guide* was published in November 1998 and provides a model for effective testing of systems for Year 2000 compliance. The testing model is divided into five levels of testing: testing infrastructure, software unit testing, software integration testing, system acceptance testing, and end-to-end testing. GAO's Year 2000 testing model presented in the guide is shown below.

GAO YEAR 2000 TESTING MODEL



Source: *Year 2000 Computing Crisis: A Testing Guide, November 1998.*